Federal Aviation Administration (FAA)

Research, Engineering and Development

Advisory Committee

Report of the Security Subcommittee

February 2002

Aviation Security Research and Development (R&D) Advisory Subcommittee

Aviation Security Technology Assessment Effort

Executive Summary

The Aviation Security R&D Advisory Subcommittee, augmented by members of the RE&D and Aviation Security Advisory Committees, met on October 25 and November 16, 2001, to address the myriad technologies proposed by the public and industry in response to the terrorist attacks of September 11, 2001. Chairman John Klinkenberg organized this Technology Assessment team into six working groups.

The working groups agreed that the United States is involved in an asymmetrical war with commercial aviation a prime target. Terrorists have transitioned commercial aircraft from a historical use as hijacker transportation or source of public attention to an expanded threat of the aircraft as a weapon of mass destruction or biological agent disseminator. The attack is not against civil aviation, but against the people and economic viability of the United States. The team agreed that we should expect more outrageous attacks than seen in the past.

In reviewing all the suggestions from industry and the public, the working groups found no "Silver Bullets." The FAA needs to adopt less than perfect approaches in the short term. These include:

- Triage procedures for screening people and their belongings;
- Focus screening resources on triage selectees;
- Harden the cockpit door;
- Demonstrate technology to screen people;
- Initiate integrated airport wide security test beds; and
- Continue to improve human performance.

In parallel with the use of these available techniques, innovative technologies for screening

people should be implemented at selected demonstration airports, where delays will not bring the air transportation system to a halt. For the long term, the FAA needs to approach aviation security as a system issue and develop technologies and techniques that allow the integration of potential threat indication information between the several threat sensing locations. Many of the recommendations and suggestions from the public and industry are for approaches that will require extensive research to demonstrate operational feasibility. Research needs to continue to identify the next generation of efficient aviation security technology. A critical threat assessment needs to be done by the FAA working with the intelligence community to identify those threats that warrant the greatest investment. Putting in place security measurers that are economically burdensome accomplishes the terrorist's objectives of crippling the U.S. economy.

Aviation Security Technology Assessment Effort

The threat to aviation security has changed, and so must our response. This report documents our assessment of technology available to combat acts of terrorism directed towards aviation security. Suggestions and recommendations were received from all sources, and the Aviation Security R&D Advisory Subcommittee evaluated these recommendations based upon the proposed technology's ability to: 1) Prevent or deter terrorists from boarding commercial aircraft or getting any type of weapon on board;
2) Prevent or deter terrorists from over powering the crew and taking control of the aircraft, if they get on board; and 3) Preserve the lives of the passengers and crew.

The Subcommittee concluded that:

- Hardening the cockpit door and bulkhead is essential;

- The FAA needs to approach aviation security as a system, with the recognition that in the short term less than perfect approaches will need to be adopted. Emphasis should be placed on identifying efficient long-term solutions;

- There are no "silver bullets." The less than perfect approaches currently being taken - or under consideration - are about the best there is;

- The huge volume of people and their belongings that need to be screened dictate a triage approach. Resources must be dedicated to screening the passengers we know the least about;

- Innovative technologies for screening people need to be implemented through several

demonstration airports where failure will not bring the total system to a halt;

- The screening of the passenger and their carry-on baggage requires both technology and human factors improvements; and

- Automated flight or airspace denial systems are not currently feasible or acceptable.

This report presents a synopsis of the recommendations of the various work groups.

RECOMMENDATIONS

Recommendation 1: Implement Test Bed Pilots

Implement test beds in two airports to demonstrate new technologies in checkpoint, checked baggage and cargo screening, access control of employees (including biometrics), perimeter intrusion, and surveillance. Integrate security systems through the implementation of centralization of command control, communication, and intelligence.

Airports must be viewed as a system. We recommend the implementation of pilot programs in two airports, one smaller (i.e. Milwaukee, WI with 6 million passengers per year) and one larger, using operations research and test bed demonstrations. This will support the rapid deployment of existing systems for screening baggage and passengers for concealed explosives and lead to the effective use of these systems. Technical and operational solutions to all security challenges should be airport tested in locations where the penalty of a mistake (airport shutdown) is minimum, i.e., start small where failure is not catastrophic. The level of protection against the breadth of threats needs to be bought up uniformly. Security operations within airports need to be integrated. Procedures and technology need to be in place to prevent, deter, or mitigate violent attacks using conventional weapons or explosives. Passenger facilitation must be part of the security solution or we will be accomplishing the terrorist's goals of paralyzing commercial aviation, and ultimately, the U.S. economy.

Technology Recommendations

Near Term (1-2 years):

We recommend applying existing technology, using either commercially available products or products near fruition with newly developed procedures and processes addressing aviation security applications. Including:

- Positively track baggage, cargo, and cabin supplies from logistics entry point to
- aircraft;
- Positively control access to the sterile areas of airport;
- Rapidly inspect all baggage for large explosive devices and dispersal mechanisms using procedures and technology;
- Test frequent flyer positive identification process and procedures;
- Verify the operational suitability of using technologies, such as biometrics and smart cards, in a Passenger Travel Identity Card; and
- Deploy anomaly detection/passenger imaging systems (x-ray or mm wave backscatter).

Recommendation 2: Enhanced Explosives Detection R&D

Perform R&D and support new detection technology development and processes that will result in efficient and effective screening in a reasonable time.

We recommend that R&D be accelerated to address the pressing need to render 100 percent screening of checked and carry on bags, and persons for weapons and explosives. There are existing technologies that can be applied to this problem, understanding that continued improvements of explosive detection and personnel screening technology need to occur.

Technology Recommendations

Near Term:

- Consider the use of combined technology to meet detection and false alarm requirements of the Explosives Detection System (EDS) certification standard.
- Consider advanced technology for screening of people such as imaging-backscatter/x-ray and trace detection portals.

Mid Term:

- Consider EDS for carry on, cargo, and mail.

Long Term (5 years):

- Develop technology for rapid inspection of all baggage and cargo for all threats.
- Develop technology for rapid inspection of all concession supplies for weapons and threat sized explosive devices.

Recommendation 3: Smart Credentials

Voluntary prescreening of trusted passengers through smart credentials. Beginning with a control pilot program, verify the operational suitability of using technologies, such as biometrics and smart cards in a Passenger Travel Identity Card. Demonstrate the use of the various models of biometrics technology for employees and passengers.

Current passenger prescreening does not assess the true identity of the passenger nor does it identify passengers who are a potential risk or threat based on historical patterns or known identification inconsistencies. Information and technology are required to assess the true identity and flag those who pose a potential risk or threat to passenger safety and security. Passengers can be identified as trusted, unknown, or name list identified. Security enhancement measures must include the following actions:

- Establish a nationwide program of voluntary prescreening of passengers, together with the issuance of "smart" credentials to trusted passengers. This will facilitate expedited processing of the vast majority of air travelers and enable security professionals to focus their resources more efficiently;
- Share relevant law enforcement and intelligence information on a continuing basis with those responsible for aviation security; and
- Deploy new technology to augment the aviation security program and ensure adequate protection for air travelers, addressing two basic categories of requirements:

    - Establishment of Identity: A Passenger Travel Identity Card could facilitate the basis in establishing identity. The passenger would apply for an Identity Card on a voluntary basis and would be subject to some form of background check as the first layer of scrutiny.

    - Determination of Trust/Risk: The passenger prescreening system is presently not linked to law enforcement or other federal agency databases, and security data is not shared between airlines when a person is transferring to/from another airline. A data interchange between federal agencies and airlines needs to be defined to share data in usable formats in a secured, timely manner.

Technology Recommendations

Near/Mid Term:

- Search and Integration of Databases

There are a number of commercially available computer programs that are designed to rapidly search various databases to verify and authenticate a person's identity. Once identity is determined (based on pre-determined data elements), the databases could be used to perform a background check and establish trustworthiness of that individual. Once identity and trust have been established, the individual would be approved for a Passenger Travel Identity Card. The card could be used within the check-in system and would, in effect, serve as evidence of prescreening for the vast majority of airline passengers, allowing security resources to be concentrated on the remaining population of travelers.

- Biometrics

Unique characteristics (fingerprint, retinal or iris scan, etc.) can be stored in the encrypted file on the Passenger Travel Identity Card. The card would be used for re-authentication of identity at check-in. The card could be used within the check-in system and would, in effect, serve as evidence.

Long Term: Expand Computer Assisted Passenger Prescreening System

Current passenger prescreening is not designed to identify passengers who are a potential risk or threat based on historical patterns or known identification inconsistencies. The passenger prescreening system is presently not linked to law enforcement or other federal agency databases, and security data is not shared between airlines when a person is transferring to/from another airline. A data interchange between federal agencies and airlines needs to be defined to share data in usable formats in a secured timely manner.

Computer Assisted Passenger Prescreening could be modified to expand the criteria (i.e., add Intel criteria, travel patterns, passport data) and application uses (scenarios for flights into or out of specific cities; i.e., DCA) to identify automatically individuals, groups, flights, and situations that necessitate extraordinary security scrutiny.

Recommendation 4: Aircraft Hardening

Incorporate aircraft hardening technologies (door and cabin) into commercial aircraft.

The primary emphasis should be on hardening cockpit doors and bulkheads. If the flight crew can be protected from hijackers getting access to the cockpit, the crew is in the best positioned to

prevent the aircraft from being used as a weapon of mass destruction. A second priority is cabin monitoring and duress alarm. However, any technology that could potentially compromise safety is unacceptable.

Technology Recommendations

Near/Mid Term:

- Aircraft Hardening:
    - Cockpit Doors and Bulkheads

The bulkhead and door must be hardened to: 1) prevent forced access; 2) be bullet resistant; and 3) withstand hand grenade attack. Reinforcing materials are available that would accomplish this, and allow the pilots to see into the cabin without being seen, and even to shoot through while being bullet resistant on the cabin side. The area around the flight deck door must be protected in flight to allow crew transit. The flight deck and flight instruments need to be protected from electronic attack (both radio frequency and electromagnetic pulse) and laser attack.

    - Aircraft Cabin

The aircraft cabin must be hardened to protect against explosive devices and their concealment. This includes designing a specific location for the placement of an explosive device discovered in flight. A hazardous material containment system must be developed for in flight use in the cabin.

- Search and Sealing Technology:

Capable people should perform aircraft searches. After cleared, the aircraft should be sealed using technology ranging from tamper proof tape to some mechanical locking device. A monitored intrusion alarm system would be a valuable addition to protecting a parked, unattended aircraft.

- Cabin Monitoring and Duress:

A duress-signaling device in the cabin to signal the cockpit in the event of a situation would be connected to remote cameras set up to monitor the cabin. Visual alert data could be communicated to the ground via cell phone technology or a form of satellite communication for over-water flights.

- Flight deviation alert to aid controllers to detect potential hijacking situations may be helpful, but needs to be considered in a broader systems context of how such information would be used to intervene.

- Taking the control of the aircraft from the pilot using automated systems is not a technically feasible or politically acceptable option at this time.

Recommendation 5: Improve Screener Performance

Accelerate R&D to enhance the tools for selection, training, and performance monitoring of screeners. Focus areas are: improved employee selection tests; advancing the implementation of Threat Image Projection (TIP); and the development of a quality management process.

The job description of airport screeners must grow to allow them to assume a greater role in the security process. Screeners are our smartest security sensor and must be offered the tools, the education, and the empowerment to perform fully their important job. We recommend the following initiatives:

- Enhance training and performance monitoring of screeners;
- Improve employee selection tests;
- Improve evaluation and performance measurers;
- Review operational procedures for human factors issues;
- Continue and advance the implementation of TIP; and
- Develop quality management process.

Additionally, we recommend background checks of all airport or airline employees and any individuals that have unescorted access to the secure areas.

Recommendation 6: Database Integration

Integrate the airport air carrier passenger database with watch list information from other government agencies. Develop the capability to track security information from curbside check-in to final gate processing.

Technology Recommendations (Near, Mid Term)

There are a number of commercially available computer programs that are designed to rapidly search various databases to verify and authenticate a passenger's identity. Once identity is

determined (based on pre-determined data elements), the databases could be used to perform a background check and establish trustworthiness of that individual. Additionally, information concerning the status of the security screens of the passenger and his/her luggage throughout the various screening stages at the airport must be coordinated, tracked, and be available to share with other, connecting airports/airlines.

Recommendation 7: Employee Access Control

Using a systems approach, incorporate technologies in access control systems, including the use of biometrics, piggyback detection, and breach control.

An integrated approach using both positive identification technologies in conjunction with access control and perimeter monitoring should be used to enforce authorized entry into the sterile environment of the airport. The challenge of an insider attack will increase as other terrorist access points are closed down.

Technology Recommendations

- Use biometrics to identify authorized airport personnel;
- Tighten control access to and all movement within the airport perimeter;
- Enhanced control, oversight, and inspection of airport ramp and catering activities; and
- Establish procedures and access control barriers/turn-stiles to deny armed personnel from forced entry beyond the hand-carry/magnetometer check points at boarding areas and at airfreight terminal.

Recommendation 8: Airport Public Area Protection

Develop procedures and evaluate and deploy as appropriate current screening technologies for truck/van/car bombs.

We recommend: the establishment of procedures, access control, and inspections to deny large explosive devices from entering the terminal; the establishment of procedures, access control, and inspections to deny car/truck bombs from approaching the terminal; an increase in security and oversight of airport ramp and catering activities, and the establishment of surveillance areas along approach and take-off paths to secure the limited areas where ground-to-air attack is probable.

Technology Recommendations

Near Term:

- Positive personnel control/turn-stiles for entry and departure from sanitized departure/ arrival areas of the airport.
- Procedures to evaluate traffic and deny car/truck bomb approach to terminal.

Long Term:

- Reconfigure airport access and terminal layouts for mitigation against truck/van/car bombs.
- Surveillance areas along approach and take-off paths to secure the limited areas where ground-to-air attack is probable.

Recommendation 9: Chem Bio Threat Technologies

Develop and/or deploy screening kits, equipment, and procedures to determine the presence or absence of chemical and/or biological warfare agents, such as anthrax, small pox, sarin, etc.

Technology Recommendations

Near Term:

- Place chemical/bio detection equipment/kits and inspection at the checkpoint.
- Develop procedures to deal with in flight release of chemical or biological agents to minimize the impact on those onboard and spread of the contamination post flights.

Long Term:

Currently no technology exists to do pre-release chemical/biological detection. Post-release detection technology is currently not fast enough to be effective in the aircraft environment. This is an important area for national long-term research.

Recommendation 10: Enhanced Cargo Screening

We recommend that more security measures be applied to inspection of cargo.

Technology Recommendations

Short Term:

- Cargo Prescreening:

We recommend a fully automated prescreening system (similar to passenger prescreening) for cargo. This system can translate complex data from shipper airway bills into plain English. This system goes far beyond the current known shipper classification. An automated cargo prescreening system could consider hazardous material shipper data, indirect air carrier data, origin/destination of shipment, flight specific instructions, and other industry information in weighted risk factors. Furthermore, there would be the opportunity to evaluate shipper data against government inter-agency watch-lists.

- Positive tracking and control of cargo and cabin supplies from entry point to aircraft.

Mid/Long Term:

Rapid inspection of all cargo for large explosive devices or other threats.

Recommendation 11: Develop a redesign of the screening checkpoint as an integrated processed engineered function incorporating features to deal with overt attempts to breach security.

Technology Recommendations:

Near/Mid Term:

- Deploy passenger imaging (x-ray backscatter or millimeter wave system) portals trace portals to look for concealed weapons or explosives on personnel;
- Increase surveillance of areas near and around the screening checkpoint;
- Establish access control barriers to prevent and contain any overt attempt by armed individuals to force a penetration of the secure area;
- Positively track all carry-on baggage, checked baggage and passengers from check-in to aircraft;
- Develop differential approach (different lanes) appropriate to the level of security screening used at checkpoint based upon the risk posed by the passenger. (Various lanes at checkpoints depending of the security risk of the passenger.);

- Use systems approach to fit the pieces (technology and procedures) together;
- Positively control access to all secure areas of the airport;

- Rapidly inspect all carry-on baggage for explosive devices and dispersal mechanism.

Long Term:

- Checkpoint redesign to integrate into airport and prevent bolters.
- Rapid inspection of all concession supplies for weapons and threat sized explosive devices.

Recommendation 12: Update, expand and refine threat analysis capability and modeling of threat mitigation measures.

Although a scant number of proposals were offered in this area, we feel that terrorists have displayed a steep learning curve of how to defeat our security. We must continue to identify terrorist threats and potential vulnerabilities in aviation security and dynamically respond to eliminate these vulnerabilities. We recommend:

- Base further security improvements on results of threat analysis and modeling of response capability;
- Develop countermeasures against cyber attack;
- Model response to hypothetical "out-of-the box" threats and tune system to meet possible threats;
- Use computer modeling to predict success of various threats;
- Develop design parameters of future airport layouts designed to offer an optimal combination of mitigation and cost effectiveness; and
- Consider protecting aircraft against electromagnetic pulse and surface to air missiles during take-off and landing.